REMARKS

This amendment is filed in response to the Office action mailed November 10, 2009. All rejections and objections are respectfully traversed.

Claims 1 – 13, 15 – 20 and 24 – 26 are pending in this case.

Claims 1, 6 – 9, 15 – 17, 20, and 24 – 26 have been amended.

No claims have been added.

Interview Summary

On January 11, 2010 the Applicant's attorney conducted a telephone interview with the Examiner. The Applicant thanks the Examiner for his time. Claim 1 and the cited references Becker-Szendy et al., U. S. Patent No. 7,243,089 (hereinafter "Becker-Szendy"), Kazar et al., U.S. Patent No. 6,868,417 (hereinafter "Kazar"), and Van Hoff et al., U.S. Patent No. 5,761,,421 (hereinafter "Van Hoff"). The Applicant's Attorney drew the Examiner's attention to the amended limitations of representative claim 1 as shown above. The Examiner stated that he would have to reanalyze the references in greater detail.

Claim Rejection – 35 USC §103

At pages 2 – 13 of the Office Action, claims 1 – 3, 6, 12 – 13, 15 – 17, 20, and 24 – 26 were rejected under 35 U.S.C. §103(a) over Becker-Szendy in view of Kazar, in further view of Van Hoff.

Applicant's claimed invention, as set forth by independent claim 1, recites:

> 1. (Currently Amended) A system comprising:
>
> a plurality of network resources configured to process received block-based protocol data access requests; and
>
> a plurality of virtual servers each allocated a logical partitioning of the network resources to establish an instance of a server comprising a processor and a memory, each virtual server configured to service the block-based data access requests by converting the block-based protocol requests to appropriate file system data requests, each virtual server further configured to share access to resources of the file system; and
>
> ***each virtual server associated with a different security domain and a context data structure including information pertaining to its***

associated security domain to enable controlled access to the allocated and shared resources of the server for that virtual server.

Becker-Szendy describes a technique for federating and migrating data in a file system using virtual servers. *See* Becker-Szendy, col. 1, lines 10 – 17. Specifically, Becker-Szendy federates a local file system into a distributed file system, while preserving local access to the existing data in the local file system. *See* Becker-Szendy, col. 2, lines 52 – 54. "Unlike most file systems, meta-data and data are stored separately in the storage tank system. The server manages meta-data comprising the location of the blocks of each file/object on shared storage." (Emphasis added). *See* Becker-Szendy, col. 3, lines 2 – 5. Further, Becker-Szendy states that metadata includes "the directory tree and the attributes of objects such as files and directories.... Typical attributes comprise … security related attributes (i.e., the identity of the owner of the object and a description of what the owner or other parties may do to the object)." *See* Becker-Szendy, col. 7, 42 – 48.

Kazar describes technique for handling file level and block level remote file accesses using the same server. *See* Kazar, Abstract. Specifically, the environment includes a network file server combined with a network block protocol server, with both servers implemented on top of inode layer abstraction. *See* Kazar, col. 3, lines 21 – 23. With respect to block level services, a block login operation passes a user ID and password and authenticates a particular user. Based upon the user, the system chooses a specific file system to which the user's block read and write operations will be applied. *See* Kazar, col. 9, line 61 – col. 10, line 1.

Van Hoff describes a technique for establishing peer-to-peer communication between computers of the same security domain. *See* Van Hoff, Abstract. During this establishment, security measures can be taken. *See* Van Hoff, col. 4, lines 35 – 36. Specifically, when establishing the peer-to-peer communication, a first virtual machine can verify that a reply packet was in fact sent by a second virtual machine by using security measures associated with a security domain that server S1, the first virtual machine, and the second virtual machine belong to. *See* Van Hoff, col. 4, lines 38 – 45. After receiving and processing the reply packet, the first virtual machine sends an

acknowledgement message to the second virtual machine and the peer-to-peer communication is established. *See* Van Hoff, col. 4, lines 48 – 51.

The Applicant respectfully submits that a combination of Becker-Szendy, Kazar, and Van Hoff does not teach or suggest the Applicant's claimed "***each virtual server associated with a different security domain and a context data structure including information pertaining to its associated security domain to enable controlled access to the allocated and shared resources of the server for that virtual server***."

The Applicant's claimed technique provides for the ability to create and maintain multiple instances of virtual servers (e.g., vfilers), within a storage system that supports block-based protocols where each vfiler is associated with a different security domain. Specifically, each vfiler is allocated dedicated and distinct units of network resources, such as volumes or qtrees, and network addresses, such as IP addresses. Each vfiler is also allowed shared access to the file system (e.g., on behalf of its clients). To accomplish this, **each vfiler, that is associated with a different security domain, is provided a context data structure** including, among other things, information pertaining to its unique associated security domain to thereby **enable controlled access to allocated and shared resources of the server for that vfiler**.

As an illustrative example, consider the following. A context data structure of a first vfiler ensures that users or clients of a first security domain can use a first set of source and destination network addresses (e.g., the allocated resources) when issuing requests to access a first subset of storage resources on a shared storage appliance. Similarly, the context data structure of a second vfiler ensures that clients of a second security domain may use a second set of source and destination network addresses (e.g., the allocated resources), that do not conflict with allocated resources dedicated to the first vfiler, to access a second subset of storage resources. Advantageously, the clients of each security domain are unaware of each other's "presence" on the storage appliance and, further, are unable to access each other's storage resources. In sum, no data flow exists between vfilers. That is, each vfiler has its own dedicated context data structure that enables controlled access to the allocated and shared resources (e.g., the file system of the server) of the server for a particular vfiler.

The Applicant notes that there appears to be agreement that Becker-Szendy and Kazar do not address this aspect of the Applicant's claim. Specifically, the Office Action states, "Becker-Szendy and Kazar do not explicitly disclose, each virtual server associated with a context data structure including information pertaining to a security domain of that virtual server to enable controlled access to the allocated and shared resources of that virtual server." *See* Office Action, pages 8 – 9.

Specifically, the Applicant notes that the metadata in Becker-Szendy simply locates information for the entire file system. Said differently, Becker-Szendy does not have a dedicated portion of metadata for each vfiler similar to the Applicant's claim that has a dedicated context data structure for each vfiler. Further, Becker-Szendy's metadata simply includes security related attributes (e.g., access rights such as read-only, and write-only). The security attributes of Becker-Szendy's metadata do not include information pertaining to a security domain **of a specific vfiler to enable controlled access to the allocated and shared resources of the server for that virtual server**. That is, the security attributes in Becker-Szendy do not apply to a specific vfiler and that vfiler's allocated and shared resources of the server for that virtual server.

Moreover, the Applicant notes that Kazar makes no mention of each vfiler of a plurality of vfilers having its own dedicated context data structure that enables controlled access to the allocated and shared resources of a server for a particular vfiler.

The Office Action suggests that Van Hoff, and specifically col. 4, lines 35 – 47, addresses this aspect of the Applicant's claim. *See* Office Action, page 9. The Applicant respectfully requests reconsideration and submits that Van Hoff simply states that two virtual machines may achieve peer-to-peer communication using security provisions (e.g., a security check). Specifically, Van Hoff states,

> Additional security provisions, such as the use of digital signatures or the like, may be added by underlying protocol layers of the communication software used by the virtual machines, for instance so that M1 can verify that the reply packet really was sent by M2. More generally, each of the virtual machines M1 and M2, operating on corresponding client computers, will use whatever communication security measures are associated with the security domain of which they and the server S1 are members and that would normally be used for communications between those virtual machines and the server S1. However, such additional

> security measures are an optional part of the operating environment in which the invention may be used. (Emphasis added). *See* Van Hoff, col. 4, lines 35 – 47.
>
> Upon receipt and processing of the reply packet P2, virtual machine M1 sends an acknowledgment message back to virtual machine M2, establishing a peer-to-peer connection between applets A1 and A2 (step 214). Thereafter, the two applets exchange messages and data (step 216) in accordance with the common security restrictions shared by the two applets. (Emphasis added). *See* Van Hoff, col. 4, lines 48 – 54.

Thus, the security check utilized between virtual machines M1 and M2 is associated with the security domain that M1, M2 and server S1 belong to. That is, the security check in Van Hoff is common among virtual machines M1 and M2 and S1. In contrast, the Applicant's claimed context data structure is associated with its own virtual server of a different security domain. Specifically, the Applicant's claims that "***each virtual server associated with a different security domain*** *and* ***a context data structure including information pertaining to its associated security domain***…." Van Hoff makes no mention of such a feature.

Further, the Applicant's claimed context data structure "***enables controlled access to the allocated and share resources of the server for that virtual server***." That is, each context data structure, that is associated with its own virtual server of a different security domain, include information for that particular virtual server that allows controlled access to allocated resources, such as network address, and shared resources, such as the file system, of the server.

For example, a first context data structure for a vfiler 1 may include information pertaining to the security domain of that vfiler 1 that indicates that vfiler 1's security domain has been allocated network addresses 1 – 10 and has access to the operating system of the file system of the server. Similarly, a second context data structure for vfiler 2 may include information pertaining to the security domain of vfiler 2 that indicates that vfiler 2's security domain has been allocated network addresses 22 – 40 and also has access to the operating system of the file system of the server.

Van Hoff makes no mention of such a feature. That is, the security check in Van Hoff does not enable controlled access to allocated and shared resources, let alone

allocated and shared resources **for a particular virtual file each of which is associated with a different security domain**. Said differently, the security check in Van Hoff does not contain information pertaining to a virtual Machine's ability to access particular allocated and particular shared resources of a server. As such, the Applicant respectfully submits Van Hoff may not fairly be interpreted to teach or suggest the Applicant's claimed "*each virtual server associated with a different security domain and* ***a context data structure including information pertaining to its associated security domain to enable controlled access to the allocated and shared resources of the server for that virtual server***."

Accordingly, Applicant respectfully urges that a combination of Becker-Szendy, Kazar, and Van Hoff is legally insufficient to render the present claims unpatentable under 35 U.S.C. 103(a)

At pages 13 – 15 of the Office Action, claims 4 – 5 and 18 – 19 were rejected under 35 U.S.C. §103(a) over Becker-Szendy in view of Kazar, in further view of Van Hoff, in further view of Mane et al., U.S. Publication No. 2005/0050107 (hereinafter "Mane").

At pages 15 – 19 of the Office Action, claims 7 – 11 were rejected under 35 U.S.C. §103(a) over Becker-Szendy in view of Kazar, in further view of Van Hoff, in further view of George et al., U.S. Patent No. 7,010,663 (hereinafter "George").

The Applicant notes that claims 4 – 5, 7 – 11, and 18 – 19 are dependent claims that depend from independent claims believed to be in condition for allowance. Accordingly, claims 4 – 5, 7 – 11, and 18 – 19 are believed to be in condition for allowance due to their dependency, as well as for other separate reasons.

Conclusion

All independent claims are believed to be in condition for allowance.

All dependent claims are dependent from independent claims which are believed to be in condition for allowance. Accordingly, all dependent claims are believed to be in condition for allowance.

Favorable action is respectfully solicited.

Please charge any additional fee occasioned by this paper to our Deposit Account No. 03-1237.

Respectfully submitted,

/Omar M. Wadhwa/

Omar M. Wadhwa
Reg. No. 64,127
CESARI AND MCKENNA, LLP
88 BLACK FALCON AVENUE
BOSTON, MA 02210
Telephone: (617) 951-2500
Facsimile: (617) 951-3927